



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,585	03/29/2004	Jeffrey A. Aaron	BELL-0340/00379 C1	2073
36072 7590 12/11/2008 AT&T Legal Department Attn: Patent Docketing Room 2A-207 One AT&T Way Bedminster, NJ 07921				
EXAMINER				
PATIL, NIRAV B				
ART UNIT		PAPER NUMBER		
2435				
MAIL DATE		DELIVERY MODE		
12/11/2008		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/811,585

**Applicant(s)**

AARON ET AL.

**Examiner**

NIRAV PATEL

**Art Unit**

2435

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 13 May 2008 (RCE).
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 29, 31-35 and 43-52 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 29, 31-35 and 43-52 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SF/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. Applicant's submission for RCE filed on May 13, 2008 has been entered. Claims 29, 31-35, 43-52 are pending.

### Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 45-52 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 45 recites "A computer readable medium comprising computer program code embodied therein configured to monitor a networked computer system when executed on a computer, the computer program code comprising: program code configured to .....". From the **specification page 14, lines 20-26** it states "...the computer-readable medium is not limited to devices such as storage device 310. For example, the computer-readable medium may include a floppy disk, a flexible disk, hard disk, magnetic tape, or any other magnetic medium, a CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, a PROM, an EPROM, a FLASH-EPROM, any other memory chip or cartridge, a **carrier wave embodied in an electrical, electromagnetic, infrared, or optical signal, or any other medium from which a computer can read...**". Based on the

cited disclosure above, it is determined that the computer readable medium carrying a signal (carrier wave) recites a non-statutory matter. Therefore, claims 45-52 are rejected under 35 USC 101.

Claims 46-52 depend on claim 45, therefore they are rejected with the same rationale applied against claim 45 above.

### **Claim Rejections - 35 USC § 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 29, 32, 33, 35, 43, 44, 45, 47, 48, 50-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US Pub. No. 2003/0110392) and in view of Sheikh et al (US Pub. No. 2002/0078382).

As per claim 29, Aucsmith discloses:

detecting an anomaly at a first device in the computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers and computer sites in the networked computer system [Fig. 1, paragraph 0037-0039, Fig. 2 step 206];

determining a second device that is anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites following the detection of the anomaly and prior to polling of the second device (i.e. possible security problem) [Fig.1, paragraph 0043-0046, 0050, 0051, 0012, 0013].

Aucsmith teaches detecting an anomaly at a first device in the computer system [Fig. 1, paragraph 0039] and determining possible security intrusions/anomaly following the detection of the anomaly at the client [paragraph 0050,0051]. Aucsmith doesn't expressively mention polling a plurality of devices of the networked computer system.

Sheikh teaches:

polling a plurality of devices of the networked computer system in a predetermined sequential order for information relating to network communication thereof [Fig. 1, 1A, paragraph 0032 lines 5-9, 0042, Fig. 4].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Sheikh with Aucsmith, since one would have been motivated to monitor the computer network systems for security purposes [Sheikh, paragraph 003].

As per claim 32, the rejection of claim 29 is incorporated and Aucsmith teaches: the anomaly comprises one of an intrusion and an intrusion attempt [paragraph 0027 lines 7-17].

As per claim 33, the rejection of claim 29 is incorporated and Aucsmith teaches:

analyzing a plurality of data packets with respect to predetermined patterns [Fig. 1, paragraph 0039].

As per claim 35, the rejection of claim 29 is incorporated and Aucsmith teaches: controlling the second device responsive to determining the second device is anticipated to be affected by the anomaly [paragraph 0012, 0013, Fig. 1].

As per claim 43, the rejection of claim 35 is incorporated and Aucsmith teaches: controlling a firewall of the second device responsive to determine the second device is anticipated to be affected by the anomaly [Fig. 1, paragraph 0054, 0057].

As per claim 44, the rejection of claim 35 is incorporated and Aucsmith teaches: Sending an alert to the second device prior to polling of the second device [Fig. 1, paragraph 0012, 0013, 0051].

As per claim 45, it encompasses limitations that are similar to limitations of claim 29. Thus, it is rejected with the same rationale applied against claim 29 above.

As per claim 47, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 32. Thus, it is rejected with the same rationale applied against claim 32 above.

As per claim 48, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 33. Thus, it is rejected with the same rationale applied against claim 33 above.

As per claim 50, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 35. Thus, it is rejected with the same rationale applied against claim 35 above.

As per claim 51, the rejection of claim 50 is incorporated and it encompasses limitations that are similar to limitations of claim 43. Thus, it is rejected with the same rationale applied against claim 43 above.

As per claim 52, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 44. Thus, it is rejected with the same rationale applied against claim 44 above.

4. Claims 31 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US Pub. No. 2003/0110392) in view of Sheikh et al (US Pub. No. 2002/0078382) and in view of Wolff et al. (US Pub. No. 2002/0174358).

As per claim 31, the rejection of claim 29 is incorporated and Aucsmith teaches that transmitting an anomaly warning from the first device to a central analysis engine, responsive to detecting the anomaly at the first device [Fig. 1, paragraph 0041 lines 1-5]. Aucsmith doesn't expressively mention that warning comprising a unique device identifier.

However, Wolff teaches that warning (i.e. report) comprising a unique device identifier [paragraph 0017 lines 1-4].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wolff with Aucsmith and Sheikh, since one would have been motivated to obtain accurate picture of anomaly and to identify a particular event and a device [Wolff, paragraph 0005 lines 1-2, 0010 lines 1-2].

As per claim 46, the rejection of claim 45 is incorporated and it encompasses limitations that are similar to limitations of claim 31. Thus, it is rejected with the same rationale applied against claim 31 above.

5. Claim 34 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aucsmith et al (US Pub. No. 2003/0110392) in view of Sheikh et al (US Pub. No. 2002/0078382) and in view of Wada et al (US Patent No. 7,047,142).

As per claim 34, the rejection of claim 33 is incorporated and Aucsmith teaches analyzing the received the data packet by the device [Fig. 1, paragraph 0025, 0039].



Wada teaches analyzing packets/data by at least two devices in the networked computer system [col. 2 lines 18-23].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Wada with Aucsmith and Sheikh, since one would have been motivated to monitor the various devices for predicting a/an failure/anomaly in the communication network [Wada, col. 1 lines 7-9].

As per claim 49, the rejection of claim 48 is incorporated and it encompasses limitations that are similar to limitations of claim 34. Thus, it is rejected with the same rationale applied against claim 34 above.

### **Response to Amendment**

6. Applicant's arguments filed May 13, 2008 have been fully considered but they are not persuasive.

Claims 45-52 have been modified to include the limitations "A computer readable medium comprising computer program code...." to correct the 35 U.S.C. 101 issue. However, the newly amended claims have not overcome such deficiency. See 35 U.S.C. 101 rejection above.

Regarding to applicant's argument to claim 29, Examiner maintains, since Aucsmith discloses that the server propagates any possible security problems seen by any of the client terminals to all of the client terminal so that all of the client terminals can defend against that possible security problem in real time. The server also uses the possible security problems reported by agent to help detect intrusion patterns, new intrusion techniques, and other security problems that may not be apparent to an individual client terminal (i.e. determining a second device that is anticipated to be affected by the anomaly .....following the detection of the anomaly and prior to detecting at the second device). Therefore, Aucsmith teaches the timing relationship as argued/claimed. Further, Sheikh's invention relates to the monitoring of computer network system for security purposes, wherein the master transport located on a center server provides for the polling of one or more agent transports (serially or parallel), which are located throughout network. The central server evaluates the report received from the agent transport. Thus, Sheikh teaches the polling mechanism in the networked computer system to obtain the report/result. In this case, the combination of Aucsmith and Sheikh teaches the claimed subject matter and the combination is sufficient to incorporate the teaching of Sheikh into the teaching of Aucsmith to utilize the polling mechanism for inspecting network traffic and identifying any anomalies or suspicious activity. The modification would be obvious because one of ordinary skill in the art would be motivated to monitor the computer network system, for security purpose, that requires minimal resistance and maximum flexibility to scalability [Sheikh, paragraph 0003, 0009].

### **Conclusion**

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to NIRAV PATEL whose telephone number is (571)272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/N. P./

*Examiner, Art Unit 2435*

/Kimyen Vu/

*Supervisory Patent Examiner, Art Unit 2435*